

عالمع ىلع رذعتي - MSS زواجت ASA 8.3: ضعف HTTP ضارعتسا بـ بـ يولـا عـقاوم

تاـيـوـتـحـمـلـا

ةـمـدـقـمـلـا

[ةـسـاسـأـلـا تـابـلـطـتـمـلـا](#)

[تابـلـطـتـمـلـا](#)

[ةـمـدـخـتـسـمـلـا تـانـوـكـمـلـا](#)

[نـيـوـكـتـلـا](#)

[ةـكـبـشـلـلـيـطـيـطـخـتـلـا مـسـرـلـا](#)

[نـيـوـكـتـ](#)

[اهـالـصـاوـاعـاطـخـأـلـا فـاشـكـتـسـا](#)

[لـحـلـا](#)

[ةـحـصـلـا نـمـقـقـحـتـلـا](#)

[ةـلـصـتـاذـتـامـوـلـعـمـ](#)

ةـمـدـقـمـلـا

لـالـخـ نـمـ بـيـوـلـا عـقاـومـ ضـعـفـ بـيـلـا لـوـصـوـلـا نـكـمـيـ اـلـ اـمـدـنـعـ ثـدـحـتـ ةـلـكـشـمـ دـنـتـسـمـلـا اـذـ فـصـيـ
ثـدـحـأـ جـمـاـنـرـبـ وـأـ 8.3ـ رـادـصـاـلـا لـغـشـيـ يـذـلـاـ (ASA)ـ فـيـكـتـلـلـ لـبـاقـلـاـ نـاـمـأـلـاـ زـاـهـ.

ةـيـاهـنـ طـاقـنـ نـمـ قـقـحـتـلـاـ اـهـدـحـأـ نـوـكـيـ،ـ ةـدـيـدـجـلـاـ نـاـمـأـلـاـ تـانـيـسـحـتـ نـمـ دـيـدـعـلـاـ ASA~7.0ـ رـادـصـاـ مـدـقـيـ
ـ ةـيـدـاعـ TCPـ ةـسـلـجـ يـفـ.ـ هـنـعـ نـلـعـمـلـاـ (MSS)ـ عـطـقـمـلـاـ مـجـحـلـىـصـقـأـلـاـ دـحـلـاـبـ مـزـتـلـتـ يـتـلـاـ
ـ نـأـ بـجـيـ SYNـ.ـ ةـمـزـحـ نـمـ TCPـ تـارـايـخـ نـمـضـ MSSـ نـيـمـضـتـ عـمـ،ـ مـدـاخـلـاـ يـلـاـ SYNـ ةـمـزـحـ لـيـمـعـلـاـ لـسـرـيـ
ـ مـثـ لـيـمـعـلـاـ ةـطـسـاـوبـ اـهـلـاـسـرـاـ مـتـ يـتـلـاـ MSSـ ةـمـيـقـ ئـلـعـ،ـ ةـمـزـحـ مـاـلـتـسـاـ دـنـعـ،ـ مـدـاخـلـاـ فـرـعـتـيـ
ـ لـ مـدـاخـلـاـوـلـيـمـعـلـاـ نـمـ لـكـ كـارـدـاـ دـرـجـمـبـ.ـ MSSـ ةـمـزـحـ يـفـ هـبـ ةـصـاخـلـاـ SYN-ACKـ.ـ ةـمـيـقـ لـسـرـيـ
ـ اـذـهـبـ صـاخـلـاـ MSSـ نـمـ رـبـكـأـ رـخـأـلـاـ يـلـاـ ةـمـزـحـ لـاـسـرـاـ عـارـظـنـلـاـ نـمـ يـأـ ئـلـعـ بـجـيـ اـلـ،ـ رـخـأـلـاـ صـاخـلـاـ
ـ رـيـظـنـلـاـ.

اهـنـعـ نـلـعـيـ يـتـلـاـ MSSـ مـرـتـحـتـ اـلـ تـنـرـتـنـاـلـاـ ئـلـعـ HTTPـ مـداـوـخـ نـمـ لـيـلـقـ دـدـعـ دـوـجـوـ فـاـشـتـكـاـ مـتـ
ـ اـهـنـعـ نـلـعـمـلـاـ MSSـ نـمـ رـبـكـأـلـاـ لـيـمـعـلـاـ يـلـاـ تـانـاـيـبـلـاـ مـزـحـ HTTPـ مـدـاخـلـسـرـيـ،ـ كـلـذـ دـعـبـوـ.ـ لـيـمـعـلـاـ
ـ رـادـصـاـ يـفـ نـاـمـأـلـاـ نـيـسـحـتـ نـيـمـضـتـ عـمـ وـ ASAـ.ـ لـالـخـ نـمـ مـزـحـلـاـ هـذـهـ بـ حـامـسـلـاـ مـتـ 7.0ـ رـادـصـاـلـاـ لـبـقـ
ـ ةـدـعـاـسـمـلـ دـنـتـسـمـلـاـ اـذـهـ بـ مـيـمـضـتـ مـتـ.ـ يـضـاـرـتـفـاـلـكـشـبـ مـزـحـلـاـ هـذـهـ طـاـقـسـاـ مـتـيـ 7.0ـ جـمـاـنـرـبـلـاـ
ـ لـيـدـبـ لـحـ ذـيـفـنـتـوـ ةـلـكـشـمـلـاـ هـذـهـ صـيـخـشـتـ يـفـ Ciscoـ نـمـ فـيـكـتـلـلـ لـبـاقـلـاـ نـاـمـأـلـاـ زـاـهـجـ لـوـفـسـمـ
ـ زـواـجـتـتـ يـتـلـاـ مـزـحـلـاـبـ حـامـسـلـلـ MSSـ.

ةـسـاسـأـلـا تـابـلـطـتـمـلـا

تابـلـطـتـمـلـا

دـنـتـسـمـلـاـ اـذـهـلـ ةـصـاخـ تـابـلـطـتـمـ دـجـوـتـ اـلـ.

ةـمـدـخـتـسـمـلـاـ تـانـوـكـمـلـا

Cisco نم (ASA) فیکتلل لباقلا نامألا زاهج ىلإ دنتسملا اذه يف ةدراولـا تامولعملـا دنتـسـتـ جـمانـربـلـا نـم 8.3 رـادـصـإـلـا لـغـشـيـيـ ذـلـكـاـ.

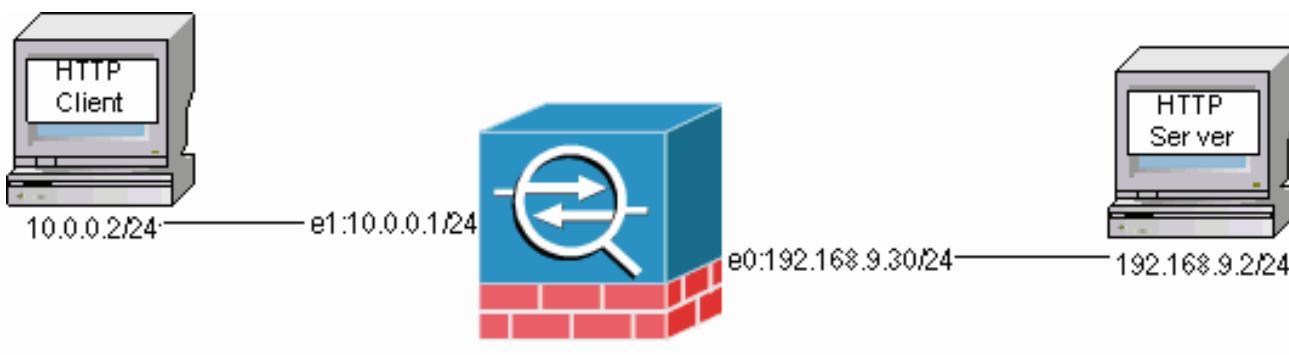
ـصـاخـ ةـيـلـمـعـ مـ ةـيـبـ يـفـ ةـدـوـجـوـمـلـاـ ةـزـهـجـأـلـاـ نـمـ دـنـتـسـمـلـاـ اـذـهـ يـفـ ةـدـرـاـوـلـاـ تـامـوـلـعـمـلـاـ عـاـشـنـإـ مـتـ تـنـاكـ اذاـ (ـيـضـارـتـفـاـ)ـ حـوـسـمـمـ نـيـوـكـتـبـ دـنـتـسـمـلـاـ اـذـهـ يـفـ ةـمـدـخـتـسـمـلـاـ ةـزـهـجـأـلـاـ عـيـمـجـ تـأـدـبـ رـمـأـ يـأـلـ لـمـتـحـمـلـاـ رـيـثـأـتـلـلـ كـمـهـفـ نـمـ دـكـأـتـفـ ،ـةـرـشـابـمـ كـتـكـبـشـ.

نـيـوـكـتـلـاـ

ـدـنـتـسـمـلـاـ اـذـهـ اـهـفـصـيـ يـتـلـاـ تـازـيـمـلـاـ نـيـوـكـتـلـاـ تـامـوـلـعـمـ مـسـقـلـاـ اـذـهـ كـلـ مـدـقـيـ

ـةـكـبـشـلـلـ يـطـيـطـخـتـلـاـ مـسـرـلـاـ

ـيـلـاتـلـاـ ـةـكـبـشـلـاـ دـادـعـاـ دـنـتـسـمـلـاـ اـذـهـ مـدـخـتـسـيـ



ـنـيـوـكـتـلـاـ ـةـA~S~A~ 8.3~

ـلـيـمـعـلـ حـامـسـلـلـ A~S~A~ 8.3~ يـضـارـتـفـاـ نـيـوـكـتـلـاـ ـىـلـاـ هـذـهـ نـيـوـكـتـلـاـ رـمـأـوـاـ ةـفـاضـاـ مـتـتـ مـداـخـبـ لـاصـتـالـاـبـ HTTP~.

ـنـيـوـكـتـلـاـ ـةـA~S~A~ 8.3~

```
ASA(config)#interface Ethernet0
ASA(config-if)#speed 100
ASA(config-if)#duplex full
ASA(config-if)#nameif outside
ASA(config-if)#security-level 0
ASA(config-if)#ip address 192.168.9.30 255.255.255.0
ASA(config-if)#exit
ASA(config)#interface Ethernet1
ASA(config-if)#speed 100
ASA(config-if)#duplex full
ASA(config-if)#nameif inside
ASA(config-if)#security-level 100
ASA(config-if)#ip address 10.0.0.1 255.255.255.0
ASA(config-if)#exit
ASA(config)#object network Inside-Network
ASA(config-obj)#subnet 10.0.0.0 255.0.0.0
ASA(config)#nat (inside,outside) source dynamic Inside-Network interface
ASA(config)#route outside 0.0.0.0 0.0.0.0 192.168.9.2 1
```

ـاـهـحـالـصـ اوـ ءـاطـخـأـلـاـ فـاشـكـتـسـاـ

فاشكـتسـالـ ئـيلـاتـلـاـ تـاوـطـخـلـاـ لـمـكـأـ،ـ لـالـخـ نـمـ نـيـعـمـ بـيـوـعـقـومـ ىـلـاـ لـوـصـولـاـ نـكـيـ مـلـ اـذـاـ فـرـعـمـ مـزـلـيـ،ـ مـزـحـلـاـ عـيـمـجـتـلـ.ـ HـT~P~ لـاـصـتـاـ نـمـ مـزـحـلـاـ طـاقـتـلـاـ ىـلـاـ الـوـأـجـاتـجـ.ـ اـهـحـالـصـ اوـ عـاطـخـأـلـاـ لـيـمـعـلـاـ ئـمـجـرـتـ مـتـتـ يـذـلـاـ IPـ نـاـوـنـعـ ىـلـاـ ئـفـاضـإـلـاـ،ـ لـيـمـعـلـاـ وـ H~T~P~ مـدـاخـلـ ـقـلـصـلـاـ تـاذـاـ نـيـوـانـعـ زـاتـجـيـ اـمـدـنـعـ هـيـلـاـ ASAـ.

يـفـ H~T~P~ لـيـمـعـ ئـجـلـاعـمـ مـتـيـوـ،ـ 192.168.9.2ـ يـفـ H~T~P~ مـدـاخـلـ لـوـانـتـ مـتـيـ،ـ لـاـثـمـلـاـ ئـكـبـشـ يـفـ.ـ ئـيـجـرـاخـلـاـ ئـهـجـاـوـلـاـ مـزـحـلـاـ كـرـتـتـ ثـيـجـ 192.168.9.30ـ ىـلـاـ H~T~P~ لـيـمـعـ نـيـوـانـعـ ئـمـجـرـتـ مـتـتـوـ،ـ 10.0.0.2ـ.ـ عـيـمـجـتـلـ نـمـ Ciscoـ (ـ فـيـكـتـلـلـ لـبـاـقـلـاـ نـاـمـأـلـاـ زـاهـجـ نـمـ طـاقـتـلـاـلـاـ ئـزـيـمـ مـادـخـتـسـاـ كـنـكـمـيـ نـكـمـيـفـ،ـ طـاقـتـلـاـلـاـ ئـزـيـمـ مـادـخـتـسـاـ ـيـوـنـتـ تـنـكـ اـذـاـ.ـ ئـيـجـرـاخـ ئـمـزـحـ طـاقـتـلـاـ مـادـخـتـسـاـ كـنـكـمـيـ وـ،ـ مـزـحـلـاـ لـوـفـسـمـلـلـ حـمـسـيـ يـذـلـاـ 7.0ـ رـاـدـصـإـلـاـ يـفـ ئـنـمـضـمـ ئـدـيـدـجـ طـاقـتـلـاـ ئـزـيـمـ مـادـخـتـسـاـ اـضـيـأـ لـوـفـسـمـلـلـ أـطـاخـ بـبـسـبـ اـهـطـافـسـاـ مـتـيـ يـتـلـاـ مـزـحـلـاـ طـاقـتـلـاـبـ TCPـ.

ةـيـنـاـكـمـلـاـ دـوـيـقـلـاـ بـبـسـبـ نـاـثـ رـطـسـ ـىـلـعـ لـوـادـجـلـاـ هـذـهـ يـفـ رـمـاـوـأـلـاـ ضـعـبـ فـتـلـتـ:ـ ئـظـحـاـلـ

1. تـاهـجـاـوـلـاـ نـمـ مـهـجـوـرـخـ وـمـهـلـوـخـ دـعـانـثـأـ مـزـحـلـاـ فـرـعـتـ يـتـلـاـ لـوـصـولـاـ مـئـاـوـقـ نـمـ جـوـزـ دـيـدـحـتـبـ مـقـ.ـ ئـيـلـخـاـدـلـاـوـ ئـيـجـرـاخـلـاـ
2. نـيـكـمـتـبـ اـضـيـأـ مـقـ.ـ نـرـاقـ يـجـرـاخـلـاـوـ ئـلـخـاـدـلـاـ عـاوـسـ دـحـ ـىـلـعـ لـقـمـسـ طـاقـتـلـاـلـاـ تـنـكـمـ
3. ئـلـعـ (ـ ASPـ)ـ عـيـرـسـلـاـ نـاـمـأـلـاـ رـاـسـمـ تـاـدـاـدـعـ حـسـمـاـ
4. ئـلـاـ هـلـاـسـرـاـ مـتـ يـذـلـاـ ئـاـطـخـأـلـاـ حـيـحـصـتـ ئـوـتـسـمـ دـنـعـ ئـمـيـاـلـمـلـلـ sysloingـ نـيـكـمـتـبـ مـقـ.ـ ئـكـبـشـلـاـ ـىـلـعـ فـيـضـمـ
5. جـارـخـاـ عـمـجـتـوـ،ـ لـكـاـشـمـلـلـ رـيـثـمـلـاـ H~T~P~ مـدـاخـلـاـ لـيـمـعـ نـمـ H~T~P~ ئـسـلـجـ أـدـبـاـ
لـاـصـتـلـاـلـاـ لـشـفـ دـعـبـ رـمـاـوـأـلـاـ هـذـهـ نـمـ تـاجـخـمـلـاـوـ
مـاظـنـلـاـ لـجـسـ ئـلـاسـرــ ئـلـاـ عـجـراـ:ـ ئـظـحـاـلـ مـاـ ئـطـاقـسـاـ رـاـهـظـاـ
outideshow capture mss-captureـ ئـلـاـ عـجـراـ:ـ ئـظـحـاـلـ مـاـ ئـطـاقـسـاـ رـاـهـظـاـ
هـذـهـ لـيـزـمـ ـىـلـعـ تـامـوـلـعـمـلـاـ نـمـ دـيـزـمـ ـىـلـعـ لـوـصـحـلـلـ 419001ـ مـقـرـ

لـحـلـاـ

يـتـلـاـ MSSـ ئـمـيـقـ زـوـاجـتـتـ يـتـلـاـ مـزـحـلـاـ طـقـسـيـ ASAـ نـأـ مـلـعـتـ ثـيـحـ نـآـلـاـ لـيـدـبـ لـحـ ذـيـفـنـتـبـ مـقـ
لـيـمـعـلـاـ ـىـلـاـ لـوـصـولـاـ مـزـحـلـاـ هـذـهـلـ حـاـمـسـلـاـ يـفـ بـغـرـتـ الـ دـقـ هـنـأـ رـكـذـتـ.ـ لـيـمـعـلـاـ اـهـنـعـ نـلـعـيـ
نـمـ مـزـحـلـاـ هـذـهـلـ حـاـمـسـلـاـ تـرـتـخـأـ هـذـهـ نـمـ تـاجـخـمـلـاـوـ
اـذـهـ لـيـدـبـلـاـ لـحـلـاـ عـاـرـجـاـ ئـعـبـاـتـمـ كـيـلـعـفـ،ـ ASAـ لـالـخـ

حـاـمـسـلـلـ هـمـاـدـخـتـسـاـ مـتـيـ 7.0ـ رـاـدـصـإـلـاـ يـفـ ئـدـيـدـجـ ئـزـيـمـ وـهـ (ـ MPFـ)ـ ئـيـطـمـنـلـاـ ئـسـاـيـسـلـاـ لـمـعـ رـاـطاـ
ـ ئـزـيـمـ لـوـحـ ئـلـمـاـكـ لـيـصـاـفـتـ عـاـرـجـاـلـ دـنـتـسـمـلـاـ اـذـهـ مـيـمـصـتـ مـتـيـ مـلـ.ـ Lـالـخـ نـمـ M~Z~H~L~A~
ـ ئـمـدـخـتـسـمـلـاـ نـيـوـكـتـلـاـ تـاـنـاـيـكـ ـىـلـاـ رـاـيـخـلـاـ نـيـكـمـتـ مـتـيـ مـلـ "ـ ئـرـادـإـلـاـ ئـوـتـسـمـ ئـاـمـحـ"
ـ ئـزـيـمـ لـوـحـ تـاـمـوـلـعـمـلـاـ نـمـ دـيـزـمـ ـىـلـعـ لـوـصـحـلـلـ 8.3ـ نـيـوـكـتـلـاـ لـلـيـلـدـ ـىـلـاـ عـجـراـ.ـ ئـلـكـشـمـلـاـ لـحلـ
ـ "ـ ئـرـادـإـلـاـ ئـوـتـسـمـ ئـاـمـحـ"ـ (ـ MPFـ)".ـ

دـرـجـمـبـ لـوـصـوـقـمـيـاـقـ رـبـعـ مـدـاـخـلـاـوـ H~T~P~ لـيـمـعـ فـيـرـعـتـ لـيـدـبـلـاـ لـحـلـاـ ـىـلـعـ ئـمـاـعـ ئـرـظـنـ نـمـضـتـتـ
ـ ئـطـيـرـخـ ـىـلـاـ لـوـصـولـاـ ئـمـئـاـقـ نـيـيـعـتـ مـتـيـوـ ئـيـفـ ئـيـفـ ئـطـيـرـخـ عـاـشـنـاـ مـتـيـ،ـ لـوـصـولـاـ ئـمـئـاـقـ دـيـدـحـتـ
ـ MSSـ زـوـاجـتـتـ يـتـلـاـ M~Z~H~L~A~ حـاـمـسـلـلـ رـاـيـخـلـاـ نـيـكـمـتـ مـتـيـوـ TCPـ ئـطـيـرـخـ نـيـوـكـتـ مـتـيـ مـلـ "ـ ئـفـلـاـ
ـ وـأـ ئـدـيـدـجـ ئـسـاـيـسـ ئـطـيـرـخـ ـىـلـاـ اـمـهـتـفـاـضـاـ كـنـكـمـيـ،ـ ئـفـلـاـ ئـطـيـرـخـ وـ TCPـ ئـطـيـرـخـ دـيـدـحـتـ درـجـمـبـ
ـ عـضـوـيـفـ service-policyـ رـمـأـلـاـ مـدـخـتـسـأـ.ـ نـاـمـأـ جـهـنـلـ جـهـنـ ئـطـيـرـخـ نـيـيـعـتـ كـلـذـ دـعـبـ مـتـيـ.ـ ئـدـوـجـوـمـ
ـ نـيـوـكـتـلـاـ تـاـمـلـعـمـ ئـفـاـضـاـ مـتـتـوـ.ـ ئـهـجـاـوـ ـىـلـعـ وـأـ مـاعـ لـكـشـبـ ئـسـاـيـسـ ئـطـيـرـخـ طـيـشـنـتـلـ نـيـوـكـتـلـاـ
ـ عـاـشـنـاـ دـعـبـ ئـفـلـاـ ئـطـيـرـخـ اـذـهـ نـيـوـكـتـلـاـ جـذـوـمـنـ فـيـضـيـ،ـ "http-map1"ـ مـسـابـ جـهـنـ ئـطـيـرـخـ
ـ جـهـنـلـاـ ئـطـيـرـخـ ـىـلـاـ ئـفـلـاـ ئـطـيـرـخـ اـذـهـ نـيـوـكـتـلـاـ جـذـوـمـنـ فـيـضـيـ،ـ

زـوـاجـتـتـ يـتـلـاـ M~Z~H~L~A~ MPFـ نـيـوـكـتـ:ـ ئـدـدـحـمـ ئـهـجـاـوـ

```

ASA(config)#access-list http-list2 permit tcp any host 192.168.9.2
ASA(config)#
ASA#configure terminal
ASA(config)#
ASA(config)#class-map http-map1
ASA(config-cmap)#match access-list http-list2
ASA(config-cmap)#exit
ASA(config)#tcp-map mss-map
ASA(config-tcp-map)#exceed-mss allow
ASA(config-tcp-map)#exit
ASA(config)#policy-map http-map1
ASA(config-pmap)#class http-map1
ASA(config-pmap-c)#set connection advanced-options mss-map
ASA(config-pmap-c)#exit
ASA(config-pmap)#exit
ASA(config)#service-policy http-map1 interface outside
ASA#

```

يـتـلـا 192.168.9.2 نـم مـزـحـلـابـ حـامـسـلـا مـتـيـ ،اهـنـاكـمـ يـفـ هـذـهـ نـيـوـكـتـلـاـ تـاـمـلـعـمـ عـضـ وـدـرـجـمـبـ وـلـوـصـوـلـاـ ـقـمـئـاـقـ نـأـ ظـحـالـمـ مـهـمـلـاـ نـمـ لـالـخـ نـمـ لـيـمـعـلـاـ ةـطـسـاـبـ اـهـنـعـ نـلـعـمـلـاـ MSSـ زـوـاجـتـتـ مـتـيـ 192.168.9.2ـ ىـلـاـ ةـرـادـاصـلـاـ رـوـرـمـلـاـ ةـكـرـحـ دـيـدـحـتـلـ ةـمـمـصـمـ ةـيـفـلـاـ ةـطـيـرـخـ يـفـ ةـمـدـخـتـسـمـلـاـ ةـرـادـاصـلـاـ SYNـ ةـمـزـحـ نـمـ جـاـرـخـتـسـاـبـ صـحـفـلـاـ كـرـحـمـلـ حـامـسـلـلـ ةـرـادـاصـلـاـ رـوـرـمـلـاـ ةـكـرـحـ صـحـفـ .ـكـانـهـ تـنـاـكـ اـذـاـ رـاـبـتـعـالـاـ يـفـ SYNـ هـاجـتـاـ عـضـوـعـمـ لـوـصـوـلـاـ ـقـمـئـاـقـ نـيـوـكـتـ يـرـوـرـضـلـاـ نـمـ ،ـكـلـذـلـ نـاـيـبـ بـمـسـقـلـاـ اـذـهـ يـفـ لـوـصـوـلـاـ ـقـمـئـاـقـ نـاـيـبـ لـادـبـتـسـاـ كـنـكـمـيـفـ ،ـاـرـاشـتـنـاـ رـثـكـأـ ـدـعـاـقـ ىـلـاـ ـجـاـجـ مـاـدـخـتـسـاـ مـتـ اـذـاـ عـيـطـبـ نـوـكـيـ نـأـ نـكـمـيـ VPNـ قـفـنـ نـأـ اـضـيـأـ رـكـذـتـ .ـعـادـأـلـاـ نـيـسـحـتـلـ TCP~MSS~ لـيـلـقـتـ كـنـكـمـيـ

يـفـ مـاعـ لـكـشـبـ ةـرـادـاصـلـاـوـ ةـدـرـاـوـلـاـ رـوـرـمـلـاـ ةـكـرـحـ نـيـوـكـتـ ىـلـعـ لـاـثـمـلـاـ اـذـهـ دـعـاـسـيـ ASA:

زـوـاجـتـتـ يـتـلـاـ مـزـحـلـابـ حـامـسـلـلـ MPFـ نـيـوـكـتـ :ـمـاعـلـاـ نـيـوـكـتـلـاـ MSS

```

ASA(config)#access-list http-list2 permit tcp any host 192.168.9.2
ASA(config)#
ASA#configure terminal
ASA(config)#
ASA(config)#class-map http-map1
ASA(config-cmap)#match any
ASA(config-cmap)#exit
ASA(config)#tcp-map mss-map
ASA(config-tcp-map)#exceed-mss allow
ASA(config-tcp-map)#exit
ASA(config)#policy-map http-map1
ASA(config-pmap)#class http-map1
ASA(config-pmap-c)#set connection advanced-options mss-map
ASA(config-pmap-c)#exit
ASA(config-pmap)#exit
ASA(config)#service-policy http-map1 global
ASA#

```

ةـحـصـلـاـ نـمـ قـقـحـتـلـاـ

جيـحـصـ لـكـشـبـ لـمـعـيـ نـيـوـكـتـلـاـ نـأـ نـمـ دـكـأـتـلـلـ اـهـمـاـدـخـتـسـاـ كـنـكـمـيـ تـاـمـوـلـعـمـ مـسـقـلـاـ اـذـهـ رـفـوـيـ

تـارـيـيـغـتـ نـأـ نـمـ قـقـحـتـلـلـ اـهـحـالـصـ اوـعـاطـخـأـلـاـ فـاـشـكـتـسـأـ مـسـقـ يـفـ ةـدـوـجـوـمـلـاـ تـاوـطـخـلـاـ رـرـكـ

هـبـ مـاـيـقـلـلـ اـهـمـيـمـصـتـ مـتـ اـمـ لـعـفـتـ نـيـوـكـتـلـاـ.

حـجـانـ لـاـصـتـاـ نـمـ Syslog

```
%ASA-6-609001: Built local-host inside:10.0.0.2
%ASA-6-609001: Built local-host outside:192.168.9.2
%ASA-6-305011: Built dynamic TCP translation from inside:10.0.0.2/58798
    to outside:192.168.9.30/1025
%ASA-6-302013: Built outbound TCP connection 13 for outside:192.168.9.2/80
    (192.168.9.2/80) to inside:10.0.0.2/58798 (192.168.9.30/1025)
%ASA-5-304001: 10.0.0.2 Accessed URL 192.168.9.2:/
```

!--- The connection is built and immediately !--- torn down when the web content is retrieved.

جاجان لاصتا نم ضرعلا رم اوأ نم جاخا

```
ASA#
ASA#show capture capture-inside
21 packets captured
1: 09:16:50.972392 10.0.0.2.58769 > 192.168.9.2.80: S
    751781751:751781751(0)
    win 1840 <mss 460,sackOK,timestamp 110313116 0,nop,wscale 0>

!--- The advertised MSS of the client is 460 in packet #1. However, !--- with the workaround in place,
packets 7, 9, 11, 13, and 15 appear !--- on the inside trace, despite the MSS>460. 2: 09:16:51.098536
192.168.9.2.80 > 10.0.0.2.58769: S 1305880751:1305880751(0) ack 751781752 win 8192 <mss 1380> 3:
09:16:51.098734 10.0.0.2.58769 > 192.168.9.2.80: . ack 1305880752 win 1840 4: 09:16:51.099009 10.0.0.2.
> 192.168.9.2.80: P 751781752:751781851(99) ack 1305880752 win 1840 5: 09:16:51.228412 192.168.9.2.80 >
10.0.0.2.58769: . ack 751781851 win 8192 6: 09:16:51.228641 192.168.9.2.80 > 10.0.0.2.58769: . ack 751781851
win 25840 7: 09:16:51.236254 192.168.9.2.80 > 10.0.0.2.58769: . 1305880752:1305882112(1360) ack 751781851
25840
8: 09:16:51.237704 10.0.0.2.58769 > 192.168.9.2.80: .
    ack 1305882112 win 4080
9: 09:16:51.243593 192.168.9.2.80 > 10.0.0.2.58769: P
    1305882112:1305883472(1360) ack 751781851 win 25840
10: 09:16:51.243990 10.0.0.2.58769 > 192.168.9.2.80: .
    ack 1305883472 win 6800
11: 09:16:51.251009 192.168.9.2.80 > 10.0.0.2.58769: .
    1305883472:1305884832(1360) ack 751781851 win 25840
12: 09:16:51.252428 10.0.0.2.58769 > 192.168.9.2.80: .
    ack 1305884832 win 9520
13: 09:16:51.258440 192.168.9.2.80 > 10.0.0.2.58769: P
    1305884832:1305886192(1360) ack 751781851 win 25840
14: 09:16:51.258806 10.0.0.2.58769 > 192.168.9.2.80: .
    ack 1305886192 win 12240
15: 09:16:51.266130 192.168.9.2.80 > 10.0.0.2.58769: .
    1305886192:1305887552(1360) ack 751781851 win 25840
16: 09:16:51.266145 192.168.9.2.80 > 10.0.0.2.58769: P
    1305887552:1305887593(41) ack 751781851 win 25840
17: 09:16:51.266511 10.0.0.2.58769 > 192.168.9.2.80: .
    ack 1305887552 win 14960
18: 09:16:51.266542 10.0.0.2.58769 > 192.168.9.2.80: .
    ack 1305887593 win 14960
19: 09:16:51.267320 10.0.0.2.58769 > 192.168.9.2.80: F
    751781851:751781851(0) ack 1305887593 win 14960
20: 09:16:51.411370 192.168.9.2.80 > 10.0.0.2.58769: F
    1305887593:1305887593(0) ack 751781852 win 8192
21: 09:16:51.411554 10.0.0.2.58769 > 192.168.9.2.80: .
    ack 1305887594 win 14960

21 packets shown
ASA#
ASA#
ASA#show capture capture-outside
21 packets captured
```

```

1: 09:16:50.972834 192.168.9.30.1024 > 192.168.9.2.80: S
    1465558595:1465558595(0) win 1840 <mss 460,sackOK,timestamp
    110313116 0,nop,wscale 0>
2: 09:16:51.098505 192.168.9.2.80 > 192.168.9.30.1024:
    S 466908058:466908058(0) ack 1465558596 win 8192 <mss 1460>
3: 09:16:51.098749 192.168.9.30.1024 > 192.168.9.2.80: .
    ack 466908059 win 1840
4: 09:16:51.099070 192.168.9.30.1024 > 192.168.9.2.80: P
    1465558596:1465558695(99) ack 466908059 win 1840
5: 09:16:51.228397 192.168.9.2.80 > 192.168.9.30.1024: .
    ack 1465558695 win 8192
6: 09:16:51.228625 192.168.9.2.80 > 192.168.9.30.1024: .
    ack 1465558695 win 25840
7: 09:16:51.236224 192.168.9.2.80 > 192.168.9.30.1024: .
    466908059:466909419(1360) ack 1465558695 win 25840
8: 09:16:51.237719 192.168.9.30.1024 > 192.168.9.2.80: .
    ack 466909419 win 4080
9: 09:16:51.243578 192.168.9.2.80 > 192.168.9.30.1024: P
    466909419:466910779(1360) ack 1465558695 win 25840
10: 09:16:51.244005 192.168.9.30.1024 > 192.168.9.2.80: .
    ack 466910779 win 6800
11: 09:16:51.250978 192.168.9.2.80 > 192.168.9.30.1024: .
    466910779:466912139(1360) ack 1465558695 win 25840
12: 09:16:51.252443 192.168.9.30.1024 > 192.168.9.2.80: .
    ack 466912139 win 9520
13: 09:16:51.258424 192.168.9.2.80 > 192.168.9.30.1024: P
    466912139:466913499(1360) ack 1465558695 win 25840
14: 09:16:51.258485 192.168.9.2.80 > 192.168.9.30.1024: P
    466914859:466914900(41) ack 1465558695 win 25840
15: 09:16:51.258821 192.168.9.30.1024 > 192.168.9.2.80: .
    ack 466913499 win 12240
16: 09:16:51.266099 192.168.9.2.80 > 192.168.9.30.1024: .
    466913499:466914859(1360) ack 1465558695 win 25840
17: 09:16:51.266526 192.168.9.30.1024 > 192.168.9.2.80: .
    ack 466914859 win 14960
18: 09:16:51.266557 192.168.9.30.1024 > 192.168.9.2.80: .
    ack 466914900 win 14960
19: 09:16:51.267335 192.168.9.30.1024 > 192.168.9.2.80: F
    1465558695:1465558695(0) ack 466914900 win 14960
20: 09:16:51.411340 192.168.9.2.80 > 192.168.9.30.1024: F
    466914900:466914900(0) ack 1465558696 win 8192
21: 09:16:51.411569 192.168.9.30.1024 > 192.168.9.2.80: .
    ack 466914901 win 14960
21 packets shown
ASA#
ASA(config)#show capture mss-capture
0 packets captured
0 packets shown
ASA#
ASA#show asp drop

Frame drop:

Flow drop:
ASA#  

!--- Both the show capture mss-capture and the show asp drop !--- commands reveal that no packets are dropped.

```

ةلص تاذ تامولعم

- [نامألا ۋەزجأ Cisco ASA 5500 Series Adaptive Security Appliances](#)
- [نام \(ASA\) ۋەزجأ كىلذىف امپ\) نامألا جىتنىمل ۋېنىادىملا تامالىعالا](#)
- [\(RFCs\) تاقىلىعتلى تابلىط](#)
- [- تادىنسىمىلى اوينقتلى معىدىلا Cisco Systems](#)

هـ لـ وـ لـ جـ رـ تـ لـ اـ هـ ذـ هـ

ةـ يـ لـ آـ لـ اـ تـ اـ يـ نـ قـ تـ لـ اـ نـ مـ مـ جـ مـ وـ عـ مـ اـ دـ خـ تـ سـ اـ بـ دـ نـ تـ سـ مـ لـ اـ اـ ذـ هـ تـ مـ جـ رـ تـ
لـ اـ عـ لـ اـ ءـ اـ حـ نـ اـ عـ يـ مـ جـ يـ فـ نـ يـ مـ دـ خـ تـ سـ مـ لـ لـ مـ عـ دـ ئـ وـ تـ حـ مـ يـ دـ قـ تـ لـ ةـ يـ رـ شـ بـ لـ اـ وـ
اـ مـ كـ ةـ قـ يـ قـ دـ نـ وـ كـ تـ نـ لـ ةـ يـ لـ آـ ةـ مـ جـ رـ تـ لـ ضـ فـ اـ نـ اـ ةـ ظـ حـ اـ لـ مـ ئـ جـ رـ يـ .ـ صـ اـ خـ لـ اـ مـ هـ تـ غـ لـ بـ
يـ لـ خـ تـ .ـ فـ رـ تـ حـ مـ مـ جـ رـ تـ مـ اـ هـ دـ قـ يـ يـ تـ لـ اـ ةـ يـ فـ اـ رـ تـ حـ اـ لـ اـ ةـ مـ جـ رـ تـ لـ اـ عـ مـ لـ اـ حـ لـ اـ وـ
ىـ لـ إـ أـ مـ ئـ اـ دـ عـ وـ جـ رـ لـ اـ بـ يـ صـ وـ تـ وـ تـ اـ مـ جـ رـ تـ لـ اـ هـ ذـ هـ ةـ قـ دـ نـ عـ اـ هـ تـ يـ لـ وـ ئـ سـ مـ
(رـ فـ وـ تـ مـ طـ بـ اـ رـ لـ اـ)ـ يـ لـ صـ أـ لـ اـ يـ زـ يـ لـ جـ نـ إـ لـ اـ دـ نـ تـ سـ مـ لـ اـ).